arXiv:1203.3162v2 [math.AG] 8 Sep 2012

ON THE GEOMETRY OF HERMITIAN ONE-POINT CODES

EDOARDO BALLICO AND ALBERTO RAVAGNANI

ABSTRACT. In this paper we study the algebraic-geometry of any one-point code on the Hermitian curve. Moreover, we characterize the minimum-weight codewords of some of their dual codes and describe many their small-weight codewords.

1. INTRODUCTION

Let q be a prime power and let $\mathbb{P}^2$ denote the projective plane over the field $\mathbb{F}_{q^2}$. Let $X \subseteq \mathbb{P}^2$ be the Hermitian curve (see [9], Example VI.3.6) of affine equation $y^q + y = x^{q+1}$. It is well-known that X is a maximal curve with q^3+1 $\mathbb{F}_{q^2}$-rational points (for instance, [8]). Let P_∞ be the only point at infinity of X, of projective coordinates $(0:1:0)$. Let $m > 0$ be an integer and let C_m be code obtained evaluating the vector space $L(mP_\infty)$ on $B := X(\mathbb{F}_{q^2}) \setminus \{P_\infty\}$. It is well-known that the dual code of C_m, here denoted by $C_m^\perp$, is $C_{m_\perp}$, with $m_\perp := q^3+q^2-q-2-m$ ([9], Theorem 2.2.8). The minimum distance of such codes has been completely determined in [10]. Table 1 gives explicit formulas for the minimum distance of any non-trivial code C_m. First of all, in Section 2 we give a geometric interpretation of the minimum distance of certain Goppa codes on arbitrary smooth curves (a geometric interpretation of the minimum distance of Goppa codes is often a key-problem in geometric coding theory). In Section 3 we describe the geometry of the minimum-weight codewords of many $C_m^\perp$ codes, extending the results of [7]. In section 4 we are going to develop some geometric tools to study even the small weight codewords of certain $C_m^\perp$ codes.

Since the Hermitian curve is a maximal one, for any $P \in X(\mathbb{F}_{q^2})$ we have an isomorphism of sheaves $\mathscr{O}_X(1) \cong \mathscr{L}((q+1)P)$, the latter one being the invertible sheaf associated to the divisor $(q+1)P$ on X. For any $m > 0$ there exists a unique pair of integers (d,a) such that $m = d(q+1) - a$ and $0 \le a \le q$. In particular we get the linear equivalence $mP_\infty \sim d(q+1)P_\infty - aP_\infty$. By setting $E := aP_\infty$, C_m turns out to be the code obtained evaluating the vector space $H^0(X, \mathscr{O}_X(d)(-E))$ on B, here denoted by $C(d,a)$. Our approach is explicitly based upon this interpretation of C_m.

1991 *Mathematics Subject Classification.* 14G15; 14H99; 14N05.

Key words and phrases. Hermitian code; Goppa code; one-point code; minimum-weight codeword; Hermitian curve.

Partially supported by MIUR and GNSAGA.

Phase	Values of m	Minimum distance
1	$0 < m < q^2 - q$ $m = \alpha q + \beta$ $0 \le \beta < q$	$q^3 - \alpha(q+1)$, if $m < q$ or $m \ge q$ and $\alpha \le \beta$ $q^3 - \beta - \alpha q$, if $m \ge q$ and $\alpha > \beta$
2	$q^2 - q \le m < q^3 - q^2$	$q^3 - m$
3	$q^3 - q^2 \le m < q^3$ $m = q^3 - q^2 + aq + b$ $0 \le a < b \le q-1$	$q^3 - m$
4	$q^3 - q^2 \le m < q^3$ $m = q^3 - q^2 + aq + b$ $0 \le b \le a \le q-1$	$q^3 - m + b$
5	$q^3 \le m \le q^3 + q^2 - q - 2$ $m_\perp = \alpha q + \beta$ $0 \le \beta < q$	$\alpha + 2$, if $m_\perp < q$ or $m_\perp \ge q$ and $\alpha \le \beta$ $\alpha + 1$, if $m_\perp \ge q$ and $\alpha > \beta$

TABLE 1. Minimum distance of any non-trivial code C_m.

2. Geometric results

We will need the following lemmas about the geometry of the Hermitian curve and certain zero-dimensional subschemes of $\mathbb{P}^2$.

Lemma 1. Let X be the Hermitian curve. Every line L of $\mathbb{P}^2$ either intersects X in $q+1$ distinct ($\mathbb{F}_{q^2}$-)rational points, or L is tangent to X at a point P (with contact order $q+1$). In the latter case L does not intersect X in any other $\mathbb{F}_{q^2}$-rational point different from P.

Proof. See [5], part (i) of Lemma 7.3.2, at page 247. □

Lemma 2. Let $X \subseteq \mathbb{P}^2$ be the Hermitian curve. Fix an integer $e \in \{2, \dots, q+1\}$ and $P \in X(\mathbb{F}_{q^2})$. Let $E \subseteq X$ be the divisor eP, seen as a closed degree e subscheme of $\mathbb{P}^2$. Let $L_{X,P} \subseteq \mathbb{P}^2$ be the tangent line to X at P. Let $T \subset \mathbb{P}^2$ be any effective divisor (i.e. a plane curve, possibly with multiple components) of degree $\le e-1$ and containing E. Then $L_{X,P} \subseteq T$, i.e. $L_{X,P}$ is one of the components of T.

Proof. Since $L_{X,P}$ has order of contact $q+1 \ge e$ with X at P, we have $E \subset L_{X,P}$. Since $\deg(E) > \deg(T)$ and $E \subseteq T \cap L_{X,P}$, Bezout theorem implies $L_{X,P} \subseteq T$. □

Lemma 3. Fix integers $d > 0$, $z \ge 2$ and a zero-dimensional scheme $Z \subset \mathbb{P}^2$ such that $\deg(Z) = z$.

(a) If $z \le d+1$, then $h^1(\mathbb{P}^2, \mathscr{I}_Z(d)) = 0$.

(b) If $d+2 \le z \le 2d+1$, then $h^1(\mathbb{P}^2, \mathcal{I}_Z(d)) > 0$ if and only if there is a line T_1 such that $\deg(T_1 \cap Z) \ge d+2$.
(c) If $2d+2 \le z \le 3d-1$, then $h^1(\mathbb{P}^2, \mathcal{I}_Z(d)) > 0$ if and only if either there is a line T_1 such that $\deg(T_1 \cap Z) \ge d+2$, or there is a conic T_2 such that $\deg(T_2 \cap Z) \ge 2d+2$.
(d) Assume $z = 3d$. Then $h^1(\mathbb{P}^2, \mathcal{I}_Z(d)) > 0$ if and only if either there is a line T_1 such that $\deg(T_1 \cap Z) \ge d+2$, or there is a conic T_2 such that $\deg(T_2 \cap Z) \ge 2d+2$, or there is a plane cubic T_3 such that Z is the complete intersection of T_3 and a plane curve of degree d.
(e) Assume $z \le 4d-5$. Then $h^1(\mathbb{P}^2, \mathcal{I}_Z(d)) > 0$ if and only if either there is a line T_1 such that $\deg(T_1 \cap Z) \ge d+2$, or there is a conic T_2 such that $\deg(T_2 \cap Z) \ge 2d+2$, or there are $W \subseteq Z$ with $\deg(W) = 3d$ and plane cubic T_3 such that W is the complete intersection of T_3 and a plane curve of degree d, or there is a plane cubic C_3 such that $\deg(C_3 \cap Z) \ge 3d+1$.

Proof. See [1], Lemma 2. □

The following result provides a cohomological characterization of any codeword of certain geometric Goppa codes on arbitrary curves.

Proposition 4. Let K be a finite field and let $X \subset \mathbb{P}^2_K$ be a smooth plane curve of degree c. Fix an integer $d > 0$, a zero-dimensional scheme $E \subset X$ and a finite subset $B \subset X(K)$ such that $B \cap E_{\text{red}} = \emptyset$. Let C be the code obtained evaluating the vector space $H^0(X, \mathcal{O}_X(d)(-E))$ at the points of B. Assume $\sharp(B) > dc$. The minimum distance of $C^\perp$ is the minimal cardinality, say s, of a subset $S \subseteq B$ of B such that $h^1(\mathbb{P}^2, \mathcal{I}_{S\cup E}(d)) > h^1(\mathbb{P}^2, \mathcal{I}_E(d))$. A codeword of $C^\perp$ has weight w if and only if it is supported by an $S \subseteq B$ such that

(1) $\sharp(S) = w$,
(2) $h^1(\mathbb{P}^2, \mathcal{I}_{E\cup S}(d)) > h^1(\mathbb{P}^2, \mathcal{I}_E(d))$,
(3) $h^1(\mathbb{P}^2, \mathcal{I}_{E\cup S}(d)) > h^1(\mathbb{P}^2, \mathcal{I}_{E\cup S'}(d))$ for any $S' \subsetneq S$.

Proof. The computation of $h^0(X, \mathcal{O}_X(d))$ is well-known. We impose that B does not intersect the support of E. The case $E = \emptyset$ is a particular case of [3], Proposition 3.1. In the general case notice that C is obtained evaluating a family of homogeneous degree d polynomials (the ones vanishing on the scheme E) at the points of B. Since X is projectively normal, the restriction map

$$\rho_d : H^0(\mathbb{P}^2, \mathcal{O}_{\mathbb{P}^2}(d)) \to H^0(X, \mathcal{O}_X(d))$$

is surjective. As a consequence the restriction map

$$\rho_{d,E} : H^0(\mathbb{P}^2, \mathcal{I}_E(d)) \to H^0(X, \mathcal{O}_X(d)(-E))$$

is surjective. Hence a finite subset $S \subseteq X(K) \setminus E_{\text{red}}$ imposes independent condition to the vector space $H^0(X, \mathcal{O}_X(d)(-E))$ if and only if S imposes independent conditions to $H^0(\mathbb{P}^2, \mathcal{I}_E(d))$. On the other hand, S imposes independent conditions to $H^0(\mathbb{P}^2, \mathcal{I}_E(d))$ if and only if $h^1(\mathbb{P}^2, \mathcal{I}_{E\cup S}(d)) = h^1(\mathbb{P}^2, \mathcal{I}_E(d))$

(here we use again that $S \cap E = \emptyset$). To get the existence of a non-zero codeword with support on S (not only with support con- tained in S) we need that the submatrix M_S of the parity-check matrix associated to C has the property that each of its submatrices obtained deleting one row have the same rank (each such row is associated to some $P \in S$ and we require that the codeword has support containing P). $\square$

Let us apply Proposition 4 to the particular case of Hermitian one-point codes.

Lemma 5. Let X be the Hermitian curve. Consider a code $C(d,a)$ of Section 1, with $d > 1$ and $0 \le a \le q$. If $a > d$ set $d' := d-1$, $a' := 0$. If $a \le d$ set $d' := d$ and $a' := a$. In any case define $E' := a'P_\infty$. Let $B := X(\mathbb{F}_{q^2}) \setminus \{P_\infty\}$. Then the code obtained evaluating the vector space $H^0(X, \mathscr{O}_X(d)(-E))$ on B (i.e. $C(d,a)$) and the code obtained evaluating the vector space $H^0(X, \mathscr{O}_X(d')(-E'))$ on B (i.e. $C(d',a')$) are the same code.

Proof. Since the restriction map $H^0(\mathbb{P}^2, \mathscr{O}_{\mathbb{P}^2}(d)) \to H^0(X, \mathscr{O}_X(d))$ is surjective, for any $S \subseteq B$ the restriction maps

$$\rho_E : H^0(\mathbb{P}^2, \mathscr{I}_{E \cup S}(d)) \to H^0(X, \mathscr{O}_X(d)(-E-S))$$

and

$$\rho_{E'} : H^0(\mathbb{P}^2, \mathscr{I}_{E' \cup S}(d)) \to H^0(X, \mathscr{O}_X(d)(-E'-S))$$

are surjective themselves. Every tangent line T_PX to X at a point $P \in X(\mathbb{F}_q)$ has order of contact $q+1$ with X at P and hence by Bezout's theorem it intersects X only at P. As a consequence $T_{P_\infty}X \cap E$ has degree a. If $a > d$ we get that every degree d homogeneous form vanishing on E vanishes also on the line $T_{P_\infty}X$, i.e. it is divided by the equation of $T_{P_\infty}X$. Since ρ_E and $\rho_{E'}$ are surjective and $B \cap T_{P_\infty}X = \emptyset$, we get that the codes obtained evaluating $H^0(X, \mathscr{O}_X(d)(-E))$ and $H^0(X, \mathscr{O}_X(d')(-E'))$, respectively, are in fact the same code. $\square$

3. Geometry of minimum-weight codewords

In this section we give a geometric characterization of the support of a minimum-weight codeword. Moreover, we describe the minimum-weight codewords of certain $C(d,a)^\perp$ codes.

Lemma 6. Let X be the Hermitian curve. Choose integers $d > 0$ and $0 \le a \le d$. Set $E := aP_\infty$. Then $h^1(\mathbb{P}^2, \mathscr{I}_E(d)) = 0$.

Proof. Assume $h^1(\mathbb{P}^2, \mathscr{I}_E(d)) > 0$. Since $a \le d$ then by Lemma 3 there exists a line $L \subseteq \mathbb{P}^2$ such that $\deg(L \cap E) \ge d+2$. Since in any case $\deg(L \cap E) \le d$ we immediately get a contradiction. $\square$

Corollary 7. Let X be the Hermitian curve. Choose integers $d > 1$ and $0 \le a \le q$ and consider the Hermitian one-point code $C(d,a)$ of Section 1. Define d', a' and E' as in Lemma 5. Let $\delta(d,a)$ be the minimum distance of $C(d,a)^\perp$.

A subset $S \subseteq B = X(\mathbb{F}_{q^2}) \setminus \{P_\infty\}$ of cardinality $\sharp(S) = \delta(d,a)$ is the support of a minimum-weight codeword of $C(d,a)^\perp$ if and only if $h^1(\mathbb{P}^2, \mathscr{I}_{E'\cup S}(d')) > 0$. Let $S \subseteq B$ with $\sharp(S) = \delta(a,b)$ and assume $2 \le \deg(E') + \sharp(S) \le 2d'+2$. Then S is the support of a minimum-weight codeword of $C(d,a)^\perp$ if and only if one of the following cases occurs.

(1) There exists a line $L \subseteq \mathbb{P}^2$ such that $\deg(L \cap (E' \cup S)) \ge d'+2$.
(2) $\deg(E' \cup S) = 2d'+2$ and $E' \cup S$ is contained in a conic $T \subseteq \mathbb{P}^2$.

Proof. Combine Lemma 6, Proposition 4 and cases (a) and (b) of Lemma 3. □

Corollary 8. Let X be the Hermitian curve. Choose integers $d > 1$ and $0 \le a \le q$ and consider the Hermitian one-point code $C(d,a)$ of Section 1. Define d', a' and E' as in Lemma 5. Let $\delta := \delta(d,a)$ be the minimum distance of $C(d,a)^\perp$ and let $S = \{P_1,\dots,P_\delta\}$ be the support of a minimum-weight codeword. Assume $2 \le \deg(E') + \sharp(S) \le \max\{2d'+2, 3d, 4d'-5\}$. There must exist a subscheme $W \subseteq E' \cup S$ with one of the following properties.

(1) $\deg(W) = d'+2$ and W is contained in a line.
(2) $\deg(W) = 2d'+2$ and W is contained in a conic.
(3) $\deg(W) = 3d'$ and W is the complete intersection of a cubic curve and a curve of degree d.
(4) $\deg(W) = 3d'+1$ and W is contained in a cubic curve.

Proof. Apply the first part of Corollary 7 and Lemma 3. □

Theorem 9. Let $C(d,a)$ be a code such that $0 < m = d(q+1) - a \le q^2 - 1$, with $d > 1$ and $0 \le a \le q$. Denote by $\delta := \delta(d,a)$ the minimum distance of $C(d,a)^\perp$. Then $\delta = d+2$ if $a = 0$, $\delta = d+1$ otherwise. Denote by A_δ the number of the minimum-weight codewords of $C(d,a)^\perp$ and set $B := X(\mathbb{F}_{q^2}) \setminus \{P_\infty\}$.

(1) If $a = 0$ or $a > d$ then $S = \{P_1,\dots,P_\delta\} \subseteq B$ is the support of a minimum-weight codeword if and only if $P_1,\dots,P_\delta$ are collinear. Moreover,
$$A_\delta = q^2\binom{q}{\delta} + (q^4 - q^3)\binom{q+1}{\delta}.$$
(2) If $0 < a \le d$ then $S = \{P_1,\dots,P_\delta\} \subseteq B$ is the support of a minimum-weight codeword if and only if $P_\infty, P_1,\dots,P_\delta$ are collinear. Moreover,
$$A_\delta = q^2\binom{q}{\delta}.$$

Remark 10. Notice that the formulas in the statement agree with those of [7].

Proof. The minimum distance $\delta = \delta(d,a)$ can be easily computed by reversing Table 1. Define E, d' and E' as in Lemma 5.

(1) If $a = 0$ then $\delta = d+2$, $E' = E = 0$ and $d' = d$. Let $S = \{P_1,\dots,P_\delta\} \subseteq B$ be a set of cardinality δ. Since $\deg(E') + \sharp(S) = d+2$, Corollary 7 says that S is the support of a minimum-weight codeword if and only if $P_1,\dots,P_\delta$ are collinear.

(2) If $a > d$ then $\delta = d+1$, $E = aP_\infty$, $E' = 0$ and $d' = d-1$. Let $S = \{P_1,...,P_\delta\} \subseteq B$ be a set of cardinality δ. Since $\deg(E') + \sharp(S) = d'+2$, Corollary 7 says that S is the support of a minimum-weight codeword if and only if $P_1,...,P_\delta$ are collinear.

(3) If $0 < a \le d$ then $\delta = d+1$, $E = aP_\infty$, $E' = E$ and $d' = d$. Let $S = \{P_1,...,P_\delta\} \subseteq B$ be a set of cardinality δ. Since $\deg(E) + \sharp(S) = a + d + 1 \le 2d+1$, Corollary 7 says that S is the support of a minimum-weight codeword if and only if $P_\infty, P_1,...,P_\delta$ are collinear (here we used Lemma 1).

To get the formulas for the number of minimum-weight codewords, observe that in any linear code two minimum-weight codewords with the same support are (non-zero) multiple one each other (by definition of linear code and minimum distance). Moreover, any non-zero multiple of a minimum-weight codeword is an other minimum-weight codeword with the same support. Hence we deduce our formulas by Lemma 1. □

It is easily seen that Theorem 9 describe all the codes $C(d,a)$ such that $d \le q-1$. Indeed, $m = d(q+1) - a \le q^2 - 1$ for any $0 \le a \le q$ if and only if $d \le q-1$. Now we study in details the case $d = q$.

Theorem 11. Let $d := q$, $0 \le a \le q$ and consider the code $C(d,a)$. Denote by $\delta := \delta(d,a)$ the minimum distance of $C(d,a)^\perp$. Let $S := \{P_1,...,P_\delta\}$ be the support of a minimum weight codeword.

(1) If $a = 0$ then $\delta = 2q+2$ and $P_1,...,P_\delta$ lie on a plane conic.
(2) If $a = 1$ then $\delta = 2q+1$ and $P_\infty, P_1,...,P_\delta$ lie on a plane conic.
(3) If $2 \le a < q$ then $\delta = 2q$ and $P_1,...,P_\delta$ lie either on the union of two distinct lines meeting at P_∞, or on a smooth conic which is tangent to the Hermitian curve X at P_∞.
(4) If $a = q$ then either it occurs one of the two cases of the previous point (3), or $qP_\infty + \sum_{i=1}^{\delta} P_i$ is the complete intersection of a plane cubic and a curve of degree q.

Proof. The minimum distance $\delta = \delta(d,a)$ can be easily found by reversing Table 1:

$$\delta(d,a) = \begin{cases} 2d+2-a & \text{if } a \in \{0,1\}, \\ 2d & \text{if } a \ge 2. \end{cases}$$

Since $d = q$, in the notations of Lemma 5 we have $E' = E = aP_\infty$ and $d' = d = q$. If $a = 0$ then $\delta = 2d+2$ and $\deg(E') + \sharp(S) = 2d+2$. By Corollary 8 there exists either a subscheme $W \subseteq S$ of degree $d+2 = q+2$ and contained in a line, or a subscheme $W \subseteq S$ of degree $2d+2 = 2q+2$ and contained in a conic. The former case must be excluded because of Lemma 1. In the latter case we have that $P_1,...,P_{2q+2}$ lie on a conic. If $a = 1$ then $\delta = 2d+1$ and $\deg(E') + \sharp(S) = 2d+2$. By Corollary 8 there exists either a subscheme $W \subseteq P_\infty \cup S$ of degree $d+2 = q+2$ and contained in a line, or a subscheme $W \subseteq P_\infty \cup S$ of degree $2d+2 = 2q+2$ and contained in a conic. The former case must be excluded because of Lemma 1. In the latter case we have that $P_\infty, P_1,...,P_{2q+2}$ lie on

a conic. Let us consider the case $a \geq 2$. We have $\delta = 2d = 2q$ and $\deg(E') + \sharp(S) = a + 2d \leq 3d - 1$ (because we assumed $a < q = d$). Hence Corollary 8 applies: either there exists a subscheme $W \subseteq aP_\infty \cup S$ of degree $d+2 = q+2$ and contained in a line, or there exists a subscheme $W \subseteq aP_\infty \cup S$ of degree $2d+2 = 2q+2$ and contained in a conic. The former case must be excluded, as in the previous cases. If $W \subseteq aP_\infty \cup \{P_1, \dots, P_{2d}\}$, $\deg(W) = 2d+2$ and W is contained in a conic T then the multiplicity of P_∞ in W, say $e_W(P_\infty)$, must be at least 2. On the other hand, if $e_W(P_\infty) > 2$ then (Lemma 2) the tangent line to X at P_∞, L_{X,P_∞}, turns out to be a component of T. In this case Lemma 1 implies that $P_1, \dots, P_{2q}$ lie on the line $T - L_{X,P_\infty}$, which contradicts Lemma 1 again. As a consequence, $e_W(P_\infty) = 2$, and we are done. Indeed, L_{X,P_∞} cannot be a component of T (use Lemma 1 twice) and so T is either the union of two lines meeting at P_∞, or a smooth conic which is tangent to X at P_∞. If $a = q$ then, by Corollary 8, we must add to the previous analysis the case $W = qP_\infty + \sum_{i=1}^{\delta} P_i$, which turns out to be the complete intersection of a cubic curve and a curve of degree $d = q$. □

4. Geometry of small-weight codewords

In this section we are going to develop some geometric tools in order to study the small-weight codewords of certain $C(d,a)^\perp$ code.

Remark 12. By Lemma 5, for any $C(d,a)$ code with $d > 1$ and $0 \leq a \leq q$ there exist integers $d' > 0$ and $0 \leq a' \leq d'$ such that $C(d,a) = C(d',a')$. Hence, from now on, we will consider only $C(d,a)$ codes with $d > 0$ and $a \leq d$.

Lemma 13. Let $d > 0$ and $0 \leq a \leq d$ be integers. Consider the Hermitian one-point code $C(d,a)$. Set $B := X(\mathbb{F}_{q^2}) \setminus \{P_\infty\}$, $E {=} aP_\infty$. Fix a subset $S \subseteq B$ and an integer $e > 0$. There exists a linear subspace of $C(d,a)^\perp$ with support contained in S if and only if $h^1(\mathbb{P}^2, \mathscr{I}_{E\cup S}(d)) \geq e$.

Proof. Set $V := H^0(X, \mathscr{O}_X(d)(-E))$ and $V(-S) := H^0(X, \mathscr{I}_{S\cup E}(d))$. Write $B = S \sqcup (B \setminus S)$ and identify $K^S = \{S \to K\}$ with $K^S \times K^{B\setminus S}$. The linear projection of K^B onto its factor K^S and the inclusion $V \hookrightarrow K^B$ induce an inclusion $V/V(-S) \hookrightarrow \mathbb{F}_q^{B\setminus S}$. Fix $f \in K^B$ with support on S. By the latter assumption we have $\sum_{P\in B} f(P)g(P) = \sum_{P\in S} f(P)g(P)$ for all $g \in K^B$. The integer $i(V,S) := \sharp(S) - h^0(X, \mathscr{O}_X(d)(-E)) + h^0(X, \mathscr{O}_X(d)(-E-S))$ is the number of independent linear relations among the evaluations of V at the points of S. Hence $i(V,B)$ is the dimension of the linear subspace of $C^\perp$ formed by the words with support on S. Lemma 6 gives that the restriction map $\rho : H^0(\mathbb{P}^2, \mathscr{I}_E(d)) \to H^0(X, \mathscr{O}_X(-E))$ is surjective. Obviously $\mathrm{Ker}(\rho) = H^0(\mathbb{P}^2, \mathscr{I}_X(d))$. Since $i(V,S)$ is the number of conditions that S imposes to $H^0(X, \mathscr{O}_X(-E))$ and $S \subset X$, we get $i(V,S) = h^0(\mathbb{P}^2, \mathscr{I}_E(d)) - h^0(\mathbb{P}^2, \mathscr{I}_{E\cup S}(d))$. Since $S \cap E = \emptyset$ and $h^1(\mathbb{P}^2, \mathscr{I}_E(d)) = 0$ (Lemma 6 again), we have $i(V,S) = h^1(\mathbb{P}^2, \mathscr{I}_{S\cup E}(d))$. □

Lemma 14. Consider a code $C(d,a)$ with $d > 0$ and $0 \leq a \leq d$. Set $E := aP_\infty$. For any integer h such that $1 \leq h \leq \binom{d+2}{2} - \deg(E)$ the smallest minimum

distance of a subcode $C_h^{\perp} \subseteq C^{\perp}$ of dimension h is the minimal cardinality of a set $S \subseteq B$ such that $h^1(\mathbb{P}^2, \mathscr{I}_{S\cup E}(d)) \ge h$.

Proof. Apply lemma 13. □

Remark 15. Let W be any projective scheme and L a line bundle on it. Fix any subscheme $E \subseteq Z$. Since Z is zero-dimensional we have $h^1(Z, \mathscr{I}_{E,Z} \otimes L) > 0$. Hence the restriction map $H^0(Z, L|Z) \to H^0(E, L|E)$ is surjective. It follows that if $h^1(W, \mathscr{I}_W \otimes L) > 0$ then $h^1(W, \mathscr{I}_Z \otimes L) > 0$.

Remark 16. For any effective divisor $T \subset \mathbb{P}^2$ and any zero-dimensional subscheme $Z \subset \mathbb{P}^2$ let $\mathrm{Res}_T(Z)$ denote the residual scheme of Z with respect to T, i.e. the closed subscheme of $\mathbb{P}^2$ with $\mathscr{I}_Z : \mathscr{I}_T$ as its ideal sheaf. We have $\deg(Z) = \deg(Z \cap T) + \deg(\mathrm{Res}_T(Z))$. If $Z = Z_1 \sqcup Z_2$ then $\mathrm{Res}_T(Z) = \mathrm{Res}_T(Z_1) \sqcup \mathrm{Res}_T(Z_2)$. If Z is reduced (i.e. if Z is a finite set) then $\mathrm{Res}_T(Z) = Z \setminus Z \cap T$. For each $d \in \mathbb{Z}$ we have an exact sequence

$$0 \to \mathscr{I}_{\mathrm{Res}_T(Z)}(d-k) \to \mathscr{I}_Z(d) \to \mathscr{I}_{Z\cap T,T}(d) \to 0, \tag{1}$$

where $k := \deg(T)$. It follows that, for each integer $i \ge 0$,

$$h^i(\mathbb{P}^2, \mathscr{I}_Z(d)) \le h^i(\mathbb{P}^2, \mathscr{I}_{\mathrm{Res}_T(Z)}(d-k)) + h^i(T, \mathscr{I}_{Z\cap T,T}(d)). \tag{2}$$

Lemma 17. Let $T \subset \mathbb{P}^2$ be any divisor of degree $k \le d+2$ and let $Z \subset T$ be any zero-dimensional scheme. Then $h^1(\mathbb{P}^2, \mathscr{I}_Z(d)) = h^1(T, \mathscr{I}_{Z,T}(d))$.

Proof. Since $Z \subset T$, we have $\mathrm{Res}_T(Z) = \emptyset$. Hence the residual exact sequence (1) becomes the exact sequence

$$0 \to \mathscr{O}_{\mathbb{P}^2}(d-t) \to \mathscr{I}_Z(d) \to \mathscr{I}_{Z,T}(d) \to 0.$$

Use the fatc that $h^1(\mathbb{P}^2, \mathscr{O}_{\mathbb{P}^2}(d-k)) = 0$ and deduce (since $d-k \ge -2$) that $h^2(\mathbb{P}^2, \mathscr{O}_{\mathbb{P}^2}(d-k)) = 0$. □

Lemma 18. Fix a line $L \subset \mathbb{P}^2$ and a set $S \subset L$. If $\sharp(S) - \sharp(L\cap S) + \deg(E) - \deg(E \cap L) \le d$, then

$$\begin{aligned} h^1(\mathbb{P}^2, \mathscr{I}_{E\cup S}(d)) &= h^1(L, \mathscr{I}_{(E\cup S)\cap L,L}(d)) \\ &= \max\{0, \deg(E\cap L) + \sharp(L\cap S) - d - 1\}. \end{aligned}$$

Proof. Since $E \cap S = \emptyset$, we have $\deg(E\cup S) = \deg(E) + \deg(S)$, $\deg(\mathrm{Res}_L(E \cup S)) = \deg(\mathrm{Res}_L(E)) + \sharp(S) - \sharp(S\cap L)$ and $\deg(L\cap(E\cup S)) = \deg(E\cap L) + \sharp(S\cap L)$. The latter equality gives $h^1(L, \mathscr{I}_{(E\cup S)\cap L,L}(d)) = \max\{0, \deg(E\cap L) + \sharp(L\cap S) - d - 1\}$, because $L \cong \mathbb{P}^1$. Since $\deg(\mathrm{Res}_L(E\cup S)) \le d$, we have $h^1(\mathbb{P}^2, \mathscr{I}_{\mathrm{Res}_L(E\cup L)}(d-1)) = 0$ ([2], Lemma 34, or [4], Remarque (i) at p. 116). Hence equation (2) gives $h^1(\mathbb{P}^2, \mathscr{I}_{E\cup S}(d)) \le h^1(L, \mathscr{I}_{(E\cup S)\cap L,L}(d))$. Since $(E\cup S)\cap L \subseteq E \cup S$, Remark 15 and Lemma 17 give $h^1(\mathbb{P}^2, \mathscr{I}_{E\cup S}(d)) \ge h^1(L, \mathscr{I}_{(E\cup S)\cap L,L}(d))$. □

Lemma 19. Let $S \subset B$ be the support of a codeword of a code $C(d,a)^{\perp}$ with $d > 0$ and $a \le d$. Set $E := aP_\infty$ and assume the existence of a plane curve T such that $h^1(\mathbb{P}^2, \mathscr{I}_{\mathrm{Res}_T(E\cup S)}(d-k)) = 0$, where $k := \deg(T)$. Then $S \subseteq T$.

Proof. Let $V(S)$ (resp. $V(S\cap T)$) be the subcode of $C(d,a)^{\perp}$ formed by the codewords whose support is contained in S (resp. in $S\cap T$). We have to prove that $V(S)=V(S\cap T)$. Obviously $V(S\cap T)\subseteq V(S)$. From (1) we get $h^1(\mathbb{P}^2,\mathscr{I}_{E\cup S}(d))=h^1(\mathbb{P}^2,\mathscr{I}_{T\cap(E\cup S)}(d))$. Hence lemma 13 applied to $S\cap T$ and to S gives $V(S)\subseteq V(S\cap T)$. □

Notation 20. We will denote by L_{X,P_∞} the tangent line to the Hermitian curve X at P_∞. $\mathscr{R}(\infty)$ will be the set of the lines passing through P_∞ which are not tangent to X in any point. $\mathscr{R}$ will denote the set of the lines which do not contain P_∞ and which are not tangent to X in any point.

The following result provides a complete description of the small-weight codewords of any code $C(d,a)$ such that $d\le q-1$ and $0\le a\le d$ (see also Remark 12).

Theorem 21. Consider a code $C(d,a)$ with $0<d\le q-1$ and $0\le a\le d$. Let $S=\{P_1,\dots,P_w\}$ be the support of a codeword of $C(d,a)^{\perp}$ of weight w.

(1) Assume the inequalities $d+2\le a+w\le 2d+1$. Then S is one of the sets in the following list.
  (a) Any subset of w elements of $L\cap B$ for an $L\in\mathscr{R}(\infty)$ ($w\ge d+1$).
  (b) Any subset of w elements of $L\cap B$ for an $L\in\mathscr{R}$ ($w\ge d+2$).
  Moreover, any such a set appears as the support of a codeword of $C(d,a)^{\perp}$ of weight w.
(2) Assume the inequalities $2d+2\le a+w\le 3d-1$. Then either S is one of the sets in cases (a), (b) of the previous list,
  (c) or there exist two distinct lines $L,M\subseteq\mathbb{P}^2$ such that
    - $\deg(L\cap(E\cup S))\ge d+2$,
    - $\deg(M\cap(E\cup S))\ge d+1$,
    - $\deg((L\cup M)\cap E)+w\ge 2d+2$,
    - either $w\ge 2d+3$ (if $L,M\in\mathscr{R}$), or $w\ge 2d+2$ (if $(L,M)\in\mathscr{R}\times\mathscr{R}(\infty)$ or $(M,L)\in\mathscr{R}\times\mathscr{R}(\infty)$), or $w\ge 2d+1$ (if $L,M\in\mathscr{R}(\infty)$),
  (d) or there exists two distinct lines $L,M\subseteq\mathbb{P}^2$ such that
    - $\deg(L\cap(E\cup S))=\deg(M\cap(E\cup S))=d+1$,
    - $\deg((L\cup M)\cap E)+w\ge 2d+2$,
    - $L\cap M\cap S=\emptyset$,
    - either $w=2d$ (if and only if $a\ge 2$, $L\cap M=P_\infty$), or $w=2d+1$ (if and only if $a\ge 1$, $(L,M)\in\mathscr{R}\times\mathscr{R}(\infty)$ or $(M,L)\in\mathscr{R}\times\mathscr{R}(\infty)$), or $w=2d+2$ (if and only if $L,M\in\mathscr{R}$),
  (e) or there exists a smooth conic $T\subseteq\mathbb{P}^2$ such that
    - $\deg(T\cap E)+w\ge 2d+2$,
    - $w\ge 2d+2-\min\{2,a\}$.

Proof. Let us divide our proof into several steps.

(1) Let $S\subseteq B$ be the support of a codeword of weight w of $C(d,a)^{\perp}$. Observe that $\sharp(S)=w$. By Proposition 4 we have $h^1(\mathbb{P}^2,\mathscr{I}_{E\cup S}(d))>0$. Assume $d+2\le a+w\le 2d+1$, i.e. $\deg(E\cup S)\le 2d+1$. By Lemma 3 there exists a line $L\subseteq\mathbb{P}^2$ (defined over $\overline{\mathbb{F}_{q^2}}$) such that $\deg(L\cap(E\cup S))\ge$

$d+2$. Since $\deg(\mathrm{Res}_L(E\cup S)) \le 2d+1-d-2 \le d$, the case $k=1$ of lemma 19 implies $S \subset L$. Since $S \ne \emptyset$ and each point of S is defined over $\mathbb{F}_{q^2}$ then also L is defined over $\mathbb{F}_{q^2}$. Set $W := L \cap (E \cup S)$ and note that the multiplicity of P_∞ in W, say $e_W(P_\infty)$, must satisfies $e_W(P_\infty) \le 1$. Indeed, if $e_W(P_\infty) \ge 2$ then Lemma 1 implies $L = L_{X,P_\infty}$, which contradicts $\deg(W) \ge d+2$ (we assumed $a \le d$). Hence we have $\sharp(L \cap S) \ge d+1$ and the support S consists of w points in $L \cap B$ for a certain $L \in \mathscr{R}(\infty) \sqcup \mathscr{R}$. On the other hand, let $L \in \mathscr{R}(\infty) \sqcup \mathscr{R}$ and let $S \subseteq B \cap L$ with $\sharp(S) = w$. Assume $a+w \le 2d+1$. Observe that $\sharp(S)-\sharp(L\cap S)+\deg(E)-\deg(E\cap L) \le w-w+a \le d$ and hence by Lemma 18 we have $h^1(\mathbb{P}^2, \mathscr{I}_{E\cup S}(d)) > h^1(\mathbb{P}^2, \mathscr{I}_{E\cup S'}(d))$ for any $S' \subsetneq S$. Apply Proposition 4 and deduce that S appears as the support of a codeword of $C(d,a)^\perp$ of weight w.

(2) Let $S \subseteq B$ be the support of a codeword of weight w of $C(d,a)^\perp$. Observe that $\sharp(S) = w$. By Proposition 4 we have $h^1(\mathbb{P}^2, \mathscr{I}_{E\cup S}(d)) > 0$. Assume $2d+2 \le a+w \le 3d-1$. By Lemma 3 there exists either a line $L \subseteq \mathbb{P}^2$ (defined over $\overline{\mathbb{F}_{q^2}}$) such that $\deg(L\cap(E\cup S)) \ge d+2$, or a plane conic T such that $\deg(T\cap(E\cup S)) \ge 2d+2$.

(2.i) Assume the existence of a line $L \subseteq \mathbb{P}^2$ such that $\deg(L\cap(E\cup S)) \ge d+2$. If $h^1(\mathbb{P}^2, \mathscr{I}_{\mathrm{Res}_L(E\cup S)}(d-1)) = 0$ then Lemma 19 implies $S \subseteq L$ and we may repeat the proof of case (A). The support S consists of w points in $L \cap B$ for a certain $L \in \mathscr{R}(\infty) \sqcup \mathscr{R}$. Every such a line gives a codeword of $C(d,a)$ of weight w. Now assume $h^1(\mathbb{P}^2, \mathscr{I}_{\mathrm{Res}_L(E\cup S)}(d-1)) > 0$. Since $\deg(\mathrm{Res}_L(E\cup S)) \le a+w-(d+2) \le 2(d-1)+1$, Lemma 3 implies the existence of a line $M \subseteq \mathbb{P}^2$ such that $\deg(M\cap\mathrm{Res}_L(E\cup S)) \ge (d-1)+2 = d+1$. We easily see that M is defined over $\mathbb{F}_{q^2}$ and not tangent to X in any point (use Lemma 1). Since $\mathrm{Res}_L(S) = S-(S\cap L)$ we get $L \ne M$. Observe that $\deg((L\cup M)\cap(E\cup S)) = \deg(L\cap(E\cup S)) + \deg(M \cap \mathrm{Res}_L(E\cup S)) \ge 2d+3$. Since neither L or M are tangent to X we have $\deg(E\cap(L\cup M)) \le 2$, with equality if and only if $L, M \in \mathscr{R}(\infty)$. In this case we have $w \ge 2d+1$ and it will be (Lemma 1) $d \le q-1$ or $d = q$ and $\deg(E\cap(L\cup M)) \le 1$. Since $\deg(\mathrm{Res}_{L\cup M}(E\cup S)) \le 3d-1-(2d+3) < d-1$, we have $h^1(\mathbb{P}^2, \mathscr{I}_{\mathrm{Res}_{L\cup M}(E\cup S)}(d-2)) = 0$ and applying Lemma 19 with $k=2$ we deduce $S \subseteq L\cup M$.

(2.ii) Assume that there is no line $L \subseteq \mathbb{P}^2$ such that $\deg(L\cap(E\cup S)) \ge d+2$. Then there is a plane conic T (not neccessairly smooth) such that $\deg(T\cap(E\cup S)) \ge 2d+2$. Since $\deg(\mathrm{Res}_T(E\cup S)) \le 3d-1-(2d+2) \le d-1$ we get $h^1(\mathbb{P}^2, \mathscr{I}_{\mathrm{Res}_T(E\cup S)}(d-2)) = 0$. Lemma 19 implies $S \subseteq T$. Assume that T is reducible, say $T = L\cup M$. Since, by assumption, $\deg(L\cap(E\cup S)) \le d+1$ and $\deg(M\cap(E\cup S)) \le d+1$ we have $L \ne M$. Since $2d+2 = \deg((L\cup M)\cap(E\cup S)) = \deg(L\cap(E\cup S)) + \deg(M\cap\mathrm{Res}_L(E\cup S))$ we get (by assumption) $\deg(L\cap(E\cup S)) = \deg(M\cap(E\cup S)) = d+1$ and $L\cap M\cap S = \emptyset$. Moreover, if P_∞ appears in $L\cap M$ then $a \ge 2$. Lemma 1 implies that neither L

or M can be tangent to X at any point. Since we assumed $a < d$ then we are done by Lemma 18. Now assume that T is smooth. Since we proved that $S \subseteq T$, Lemma 2 gives $w = \deg(T \cap S) \geq 2d + 2 - \min\{2, a\}$.

The proof is concluded. □

References

[1] E. Ballico, A. Ravagnani, *On Goppa Codes on the Hermitian Curve*. `http://arxiv.org/abs/1202.0894`.

[2] A. Bernardi, A. Gimigliano, M. Idà, *Computing symmetric rank for symmetric tensors*. J. Symbolic. Comput. **46**(1), 34–53 (2011).

[3] A. Couvreur, *The dual minimum distance of arbitrary dimensional algebraic-geometric codes*. J. Algebra **350**(1), 84–107 (2012).

[4] Ph. Ellia, Ch. Peskine, *Groupes de points de* $\mathbf{P}^2$*: caractère et position uniforme*. Algebraic geometry (L'Aquila, 1988), 111–116, Lecture Notes in Math., 1417, Springer, Berlin, 1990.

[5] J. W. P. Hirschfeld, *Projective Geometries over Finite Fields*. Clarendon Press, Oxford, 1979.

[6] J. W. P. Hirschfeld, G. Korchmáros, F. Torres, *Algebraic Curves over a Finite Field*. Princeton University Press, 2008.

[7] C. Marcolla, M. Pellegrini, M. Sala *On the weights of affine-variety codes and some Hermitian codes*. WCC 2011 - Workshop on coding and cryptography, 273–282 (2011).

[8] S. A. Stepanov, *Codes on Algebraic Curves*. Springer, 1999.

[9] Stichtenoth, *Algebraic function fields and codes*, Second Edition. Springer-Verlag, 2009.

[10] K. Yang, P. V. Kumer, *On the True Minimum Distance of Hermitian Codes*. Coding Theory and Algebraic Geometry (Stichtenoth and Tsfasman editors), Springer-Verlag, 1992.

DEPT. OF MATHEMATICS, UNIVERSITY OF TRENTO, 38123 POVO (TN), ITALY
E-mail address: `ballico@science.unitn.it`

UNIVERSITY OF TRENTO, 38123 POVO (TN), ITALY
E-mail address: `alberto.ravagnani88@gmail.com`